

SAO91 (Rev. 5/85) Criminal Complaint

UNITED STATES DISTRICT COURT

CLERK'S OFFICE U.S. DIST. COURT
AT ROANOKE, VA
FILED

DISTRICT OF

JUN 11 2009

JOHN F. CONCORAN, CLERK
BY: 
DEPUTY CLERK

UNITED STATES OF AMERICA

V.

Jeffrey L. Weaver

Roanoke, Virginia

CRIMINAL COMPLAINT

Case Number:

709m270

(Name and Address of Defendant)

I, the undersigned complainant being duly sworn state the following is true and correct to the best of my knowledge and belief. On or about January 5, 2009 in the City of Roanoke county, in the Western District of Virginia defendant(s) did, (Track Statutory Language of Offense)

with transmitting, in interstate commerce, communications on January 5, 2009, January 7, 2009, and January 10, 2009, to threaten injuries to a former Bay Area Rapid Transit (BART) police officer and a Martinsville, Virginia police officer.

in violation of Title 18 United States Code, Section(s) 875(c)

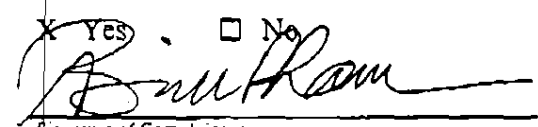
I further state that I am a(n) Special Agent of the FBI and that this complaint is based on the
Official Title

following facts:

See attached Affidavit

Continued on the attached sheet and made a part hereof:

☒ Yes ☐ No


Signature of Complainant

Sworn to before me and subscribed in my presence via telephone between Roanoke VA and
Mount Joy PA

May 29, 2009

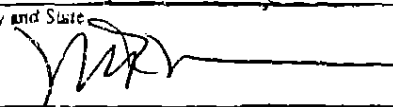
MICHAEL FURBANISHI

US MAGISTRATE JUDGE

Name and Title of Judicial Officer

at

mt. Joy, PA
City and State


Signature of Judicial Officer

270

APPLICATION AND AFFIDAVIT FOR AN ARREST WARRANT

I, Binh T. Pham, a Special Agent (SA) of the Federal Bureau of Investigation (FBI), being duly sworn, hereby depose and state as follows:

I. INTRODUCTION

1. I have been a Special Agent of the FBI for approximately four years. Since April 2006, I have been assigned to a Computer Crimes Squad of the San Francisco Division of the FBI, the primary mission of which is to investigate crimes involving computer intrusions, frauds facilitated through the use of computers, and other computer-related federal violations including death threats made on the Internet.

2. I have conducted investigations involving the use of computers and the Internet by one individual to make death threats or threats of bodily injuries against another. I have received training and gained experience in interviewing and interrogation techniques, arrest procedures, search warrant applications, the execution of searches and seizures, computer crimes and other computer-based crimes, computer evidence identification, computer evidence seizure and processing, and various other criminal laws and procedures. I have personally participated in the execution of search warrants involving the search and seizure of computer equipment and I have reviewed digital evidence collected via executions of search warrants.

3. This application is being submitted in support of an application for a warrant authorizing the arrest of JEFFREY WEAVER for violations of Title 18, United States Code (U.S.C.), § 875(c) (transmitting a communication in interstate commerce to threaten injury to another person). Based on my investigation and the investigation of other FBI Agents, I believe that WEAVER communicated direct threats from a computer located at his residence [REDACTED] Roanoke, Virginia, to a person in California and a person in Virginia.

4. The information set forth in this affidavit is based on my personal knowledge of the

①

mbr
5-29-09

270

investigation, my training and experience, information received from other FBI Special Agents, the analysis of public documents and documents obtained in the course of the investigation (including information available on the Internet), and special investigative techniques.

5. This affidavit is submitted for the limited purpose of obtaining an arrest warrant for WEAVER. I have not included each and every fact known to me concerning this investigation. I have set forth only facts that I believe are necessary to establish probable cause that WEAVER has violated Title 18, U.S.C., §§ 875(c).

II. RELEVANT STATUTES

6. According to Title 18, U.C., § 875(c), whoever "transmits in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another, shall be fined under this title or imprisoned not more than five years, or both."

III. BACKGROUND INFORMATION REGARDING COMPUTERS AND NETWORKS

7. Based upon my training, education, experience, and information told to me by other investigators experienced in the investigations of computer crimes, I have learned the following regarding computers, networks, and computer hackers.

8. An operating system (OS) is a special program that controls the way the computer, keyboard, screen, and disks work together. It is a foundation of computer software that allows the user to interact with a computer system.

9. Data that is processed by a computer may be written to the computer hard drive or other storage medium even if the user does not intentionally save the information. For example, a computer operating system may take random data out of working memory and use it to "pad" files on a computer hard drive during the storage process.

10. Electronic information can remain on computer storage media, such as hard drives, for an indefinite period of time. Even when a computer user attempts to delete records from a computer storage medium, the records may still exist and be recovered through computer forensic techniques.

(2)

JMT
5-29-09

270

11. Computer System Administrators typically conduct periodic backups of computer systems and save the backup data to digital media in the form of floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, thumb drives, micro-drives, cell phones and personal digital assistants, in order to protect data from corruption or destruction.

12. Computer files may be easily moved from computer to computer using direct wire connections, through the use of storage media such as floppy diskettes, or over a network, such as the Internet.

13. A network is a system of interconnected computer systems and terminals. A network can be configured to be accessible from another computer not normally considered part of the network. This connectivity allows data to be stored and exchanged between computers remotely.

14. Computers connected to a network have individual addresses. These addresses, in some cases known as Internet Protocol (IP) addresses, identify the computers attached to a network. In other cases, these addresses are known as NetBIOS names or addresses. An IP address is a unique code given to a computer when connected to the Internet through an Internet Service Provider (ISP). The IP address is assigned to an end user by an ISP. The IP address, along with the date and time, usually allows the ISP to identify the location of the end user and/or subscriber. An IP address looks like a series of four numbers, each in the range of 0-255, separated by periods (e.g., 121.56.97.178).

15. Access to a network at a business is typically restricted to individuals with a specific job requirement that necessitates use of the network. Access control is accomplished through the assignment of user accounts. An account can be assigned a name that identifies the account as belonging to a specific individual. Control is further restricted by the use of passwords that allow access to only the legitimate account holder or other individuals with knowledge of both the account and associated password.

16. Computers can create files, called logs, that contain a record of the time, date, and point

(3)

mdu
5-29-09

270

of origin of an individual gaining access to a computer network from a remote computer not part of the network.

17. The Internet connects individual computers and networks into a large worldwide network. The Internet makes it possible for computers, located great distances apart, to be connected to each other.

18. The term "computer," as used herein, is defined pursuant to 18 United States Code, Section 1030(e)(1) as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device."

IV. SUMMARY OF PROBABLE CAUSE TO SEARCH THE SUBJECT PREMISES

19. On January 1, 2009, former San Francisco Bay Area Rapid Transit (BART) police officer Johannes Mehserle, while on duty, was involved in a controversial shooting resulting in the death of Oscar Grant, a subject who was being restrained at the time he was shot. In the days that followed, the incident received significant media attention and prompted protests in the Bay Area. On January 8, 2009, Todd Mehserle, Officer Mehserle's father, contacted the San Francisco Division of the FBI and reported that he had found death threats against his family posted on the Internet. Specifically, Mr. Mehserle advised that the threats were posted on a web site located at URL www.infowars.com (INFOWARS). One of the threats contained Mr. Mehserle's home address.

20. On January 13, 2009, your Affiant visited INFOWARS and identified two web pages containing Mr. Mehserle's home address. The first web page was located at URL http://www.infowars.com/?p=6696&cp=all#comments. This web page contained excerpts from a newspaper article purportedly written by the Associated Press and titled "Family of man killed by BART officer plans to sue." The excerpts summarized the aforementioned New Year's Day shooting.

(4)

mm
5-29-09

270

Following the excerpts were comments posted by visitors to the web page that addressed the New Year's Day shooting. Each comment was identified by the date and time when it was posted and the name or identity used by the individual who posted the comment.

21. On January 5, 2009, at approximately 5:00 p.m., an individual using the identity "FuckThePIGS" posted the following comment to the above-referenced news story concerning the New Year's Day shooting: "FUCK THE PIGS AND IF I FIND OUT WHO THE PIG IS THEN I WILL KILL THE PIG WHO KILLED HIM." This threat is hereinafter referred to as THREAT #1.

22. Approximately 12 minutes later, the user identified as *FuckThePIGS* posted another comment - referred to herein as THREAT #2 - to the above-referenced news story, which read as follows:

The best pigs are dead fucking pigs and if any of you Oakland or BART pigshit fuckers are reading this your time is coming you pigshit muthafuckers sooner then you think and this isn't a threat its a fucking promise bitches!!! Im curious to know what it looks like up close to see pigshit fuckers get their brains splattered against a wall. [sic]

23. A second web page, this one containing Mr. Mehserle's home address, was located at URL <http://www.infowars.com/?p=7007&cp=all#comments>. This web page contained a video titled "Video: BART Cop Execution" along with comments posted by visitors. On January 7, 2009, at approximately 7:10 p.m., an individual using the same identity of *FuckThePIGS* posted death threats against officer Mehserle and his family. These threats are hereinafter referred to as THREAT #3. The threats read:

Officer Johannes Mehserle, [home address omitted], CALIFORNIA [zip code omitted]

IS GOING TO BE A DEAD PIGSHIT MUTHAFUCKER NOW. THANKS FOR THE ADDRESS OF THE STUPID PIGSHIT FUCKER NOW THAT I KNOW WHO HE IS AND WHERE HE IS ITS ONLY A MATTER OF TIME AND HIS PUNISHMENT WILL BE TO WATCH HIS BITCH AND HIS BABY GET WASTED IN FRONT OF HIM AND THEN HE JOINS THE BITCH AND THE BABY IN HELL WHEN I FINISH THE JOB BY WASTING HIS PIGSHIT FUCKING ASS. THIS ISN'T A THREAT ITS A FUCKING PROMISE TO ALL YOU PIGSHIT LOVERS AND HATERS BECAUSE JUSTICE WILL BE SERVED DEATH WISH CHARLES BRONSON VIGILANTE STYLE AND REVENGE IS A DISH BEST SERVED COLD. FUCK THE PIGS THE BEST PIGS ARE DEAD PIGS.

5

5-29-09

270

24. Free Speech Systems, LLC, the administrator of INFOWARS, whose headquarters is located in Austin, Texas, provided records showing that THREAT #1 and THREAT #2 were posted from IP address 151.199.13.106 and THREAT #3 was posted from IP address 70.100.0.162. Additionally, the INFOWARS administrator advised that the time zone associated with the comments was recorded as Eastern Standard Time (EST). According to publicly-accessible information, the Internet Service Provider (ISP) for IP addresses 151.199.13.106 and 70.100.0.162 is Verizon Online.

25. Records provided by Verizon Online showed IP address 151.199.13.106 was assigned to Verizon account number [REDACTED] from January 5, 2009, at 0031 Greenwich Mean Time (GMT) to January 6, 2009, at 0142 GMT. According to your Affiant's calculation, this time range is January 4, 2009, at 7:31 p.m. EST to January 5, 2009, at 8:42 p.m. EST.

26. IP address 70.100.0.162 was also assigned to Verizon account number [REDACTED]. The IP address was assigned to the account from January 7, 2009, at 0508 GMT to January 9, 2009, at 1856 GMT. According to your Affiant's calculation, this time range is January 7, 2009, at 12:08 a.m. EST to January 9, 2009, at 1:56 p.m. EST.

27. IP address 70.100.0.162 was also assigned to Verizon account number [REDACTED] from January 10, 2009, at 0910 GMT to January 12, 2009, at 1015 GMT. According to your Affiant's calculation, this time range is January 10, 2009, at 4:10 a.m. EST to January 12, 2009, at 5:15 a.m. EST.

28. Verizon records showed that the account holder of account number [REDACTED] JEFFREY WEAVER, [REDACTED] Roanoke, Virginia 24017 (the SUBJECT PREMISES).

29. According to INFOWARS's records, IP address 70.100.0.162 was also used by the username *FuckThePIGS* to post a message threatening to shoot a Martinsville, Virginia, police officer with a 9 mm pistol. The message was posted in response to a newspaper article reporting an incident involving a Martinsville, Virginia, police officer who used a taser gun on a 17-year-old person resulting

(6)

W
5-29-09

MAY-29-2009 17:29

FBI ROANOKE

P.02

270

in that person's death. The message, posted on January 10, 2009, at 3:46 p.m. EST, stated:

All I got to say is that I'm within 100 miles of where this incident happened at and reading this makes my blood boil. Maybe I should drive to Martinsville with my 9mm Glock and some teflon coated armor piercing Black Rhino hollow point rounds and do the world a favor by ridding the world of this piece of shit pig...

30. On May 29, 2009, your Affiant and other agents executed an authorized search warrant at WEAVER's residence, [REDACTED], Roanoke, Virginia. During this interview, your Affiant and Special Agent David Frey confronted WEAVER regarding the messages referenced above in paragraphs 19 through 29. WEAVER admitted he frequents INFOWARS and he was angry when he made these postings. WEAVER acknowledged posting these messages, but stated he did not intend to harm anyone.

VI. CONCLUSION

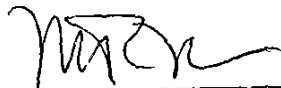
31. Based on all of the facts and circumstances described above, your Affiant submits that there is probable cause to believe that JEFFREY WEAVER transmitted threatening communications in violation of Title 18, U.S.C., § 875(c).

32. Your Affiant respectfully requests that a warrant be issued to authorize the arrest of JEFFREY WEAVER.



Binh T. Pham
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me ^{telephonically} this 29th day of May, 2009.



Michael F. Urbanski
UNITED STATES MAGISTRATE JUDGE

(7)

TOTAL P.02